UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF OHIO EASTERN DIVISION

IN RE: NATIONAL PRESCRIPTION OPIATE LITIGATION	)	**MDL No. 2804**
	)	**Case No. 1:17-md-2804**
THIS DOCUMENT RELATES TO: Track One-B Cases	)	**Judge Dan A. Polster**

WALGREENS' MOTION FOR A PROTECTIVE ORDER

Plaintiffs refuse to destroy private patient prescription data that Walgreens inadvertently produced—data the Court has already ordered is ***not*** subject to discovery. Plaintiffs offer no justification for retaining this data, nor could they, given the Court's prior order. Plaintiffs' intransigence puts thousands of highly sensitive patient prescription records at risk of an unnecessary data breach. Courts routinely order the destruction of inadvertently produced sensitive data. The Court should exercise its broad discretion under Federal Rule 26(c) to enter such an order here.

BACKGROUND

On Monday, March 2, 2020, Walgreens produced an encrypted hard drive containing dispensing data for Cuyahoga and Summit Counties to Peter Weinberger's attention at Spangenberg Shibley & Liber. Ex. 1, Email: Walgreens – Ohio Dispensing Data (March 2, 2020). Walgreens produced this data over objections, to comply with this Court's orders, and reserved all rights to object to the use of the data at trial or otherwise. *Id*. The Court specifically restricted the timeframe for discoverable dispensing data to 2006 to the present, and rejected Plaintiffs' request for data dating back to 1996. *See* Dkt. 3055 at 4 n.2. Walgreens produced the data pursuant to the protective orders in this case and marked it Highly Confidential and Confidential Protected Health Information under those orders. *Id*.

Shortly after making this production, Walgreens determined it had inadvertently included private dispensing data for prescriptions prior to 2006 due to a vendor error more fully explained below.

Immediately upon making this discovery, Walgreens contacted Plaintiffs' counsel and requested that they destroy the pre-2006 data. Ex. 2, Email: Re: Walgreens – Ohio Dispensing Data (March 7, 2020); Ex 3, Aff. of Hannah Hamburger ("Hamburger Aff."), at 1-2. In response, Plaintiffs did not claim that the data was relevant in any way—or even discoverable. Instead, Plaintiffs said that the data was not subject to clawback and refused to destroy it. As a result, Walgreens now must seek a protective order from this Court.

ARGUMENT

This Court "may, for good cause, issue an order to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." Fed. R. Civ. P. 26(c).

The decision whether to grant a request for a protective order is "entrusted to the district court's sound discretion." *Microsoft Corp v. Commonwealth Scientific and Indus. Research Organisation*, 2009 WL 440608, at *1 (E.D. Texas Feb. 23, 2009) (citing *Nguyen v. Excel Corp*., 197 F.3d 200, 209 n. 27 (5th Cir. 1999)).

In determining whether to issue a protective order, courts weigh the risk from inadvertent disclosure against the receiving party's need for the information to prosecute or defend its claims. *See Microsoft Corp*. 2009 WL 440608 at *2 (citation omitted); *see also Heriot v. Byrne*, 257 F.R.D. 645, 660-661 (N.D. Ill. 2009) (ordering clawback of inadvertently produced privileged documents where producing party took reasonable precautions to prevent disclosure and promptly sought to rectify the error).

Here, the risk from disclosure is high. A data breach of this sensitive patient data would

reveal the private and personal information of a large number of patients. In addition, Walgreens took precautions that were beyond reasonable to avoid disclosure—actions that lend further support to Walgreens' request. Plaintiffs' "need" for the data, on the other hand, is nonexistent. Indeed, the Court already has ordered that the data in question was not even subject to discovery. This balance requires that the inadvertently produced data be destroyed.

First, the inadvertently disclosed patient prescription information is unquestionably sensitive and highly confidential. These patient records include information not just about the specific opioid, drug strength, and dosage a patient took, but also the patient's zip code, diagnosis, and whether he or she was taking other medications at the same time.[1]

The risk from disclosure of that information is high. Although Walgreens made significant efforts to anonymize the data, *see* Ex. 3, Hamburger Aff. ¶ 13, it is well known that large datasets of this kind are susceptible to re-identification. *See*, e.g., Stuart A. Thompson and Charlie Warze, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. Times (Dec. 19, 2019) (reporting that the *New York Times* succeeded in matching purportedly anonymous cell phone data with specific individuals). That risk is heightened here in light of the long list of data fields Walgreens was ordered to produce. *See* Dkt. 3106 at Ex. A (listing 34 data fields that were required to be produced with Walgreens' dispensing data).

Even assuming best efforts and good faith, Plaintiffs and their counsel are unlikely to be equipped to properly secure these records to prevent a data breach. Moreover, once disclosed to government entities, this data may become subject to public records requests under different

[1] Because of the sensitivity of this information, the Pharmacy Defendants did not request fields such as patient address or diagnosis from the Ohio Board of Pharmacy when the Pharmacies moved to compel certain other limited data from the Board's OARRS database that is necessary to defend against Plaintiffs' claims.

state-law legal standards. *See In re Nat'l Prescription Opiate Litig*., 927 F.3d 919, 926, 931 (6th Cir. 2019). There is no way to guarantee that future disclosure will be prevented. To be clear, this is a concern with respect to ***all*** of the dispensing data Walgreens produced. But here, Plaintiffs have refused to destroy data that the Court has deemed ***is not even discoverable***. Plaintiffs have offered no justification for allowing them to retain this data because there is no such justification.

In cases like this, courts exercise their discretion to order the destruction of the data in question. For example, in *In re Incretin-Based Therapies*, 2015 WL 5566287 at *1 (S.D. Cal. Sep. 11, 2015), Plaintiffs refused to return inadvertently produced potentially sensitive medical data. The Court determined that even though the data was "not subject to any particular privilege, the data is still proprietary and sensitive" and the risk of further inadvertent disclosure was high. *Id.* at *1. As a result, the Court ordered the parties to strike any reference to the data in expert reports, ordered the Plaintiffs to destroy or return all copies of the data in their possession or contained in their expert files, and to submit a declaration verifying such action. *Id.* at *1; *see Henry v. Ocwen Loan Servicing, LLC*, 2018 WL 1638255 at *3 (S.D. Cal. Apr. 5, 2018) (ruling that "[c]onfidential servicing notes," while not privileged or otherwise protected, must be returned or destroyed in order to mitigate the risk of further disclosure); *Microsoft Corp*., 2009 WL 440608, at *3 (issuing protective order preventing use of confidential information in negotiations because "Cisco's risk of inadvertent disclosure or misuse of its confidential documents outweighs CSIRO's need for the material to prosecute it case").

Second, Walgreens' good faith is apparent from the substantial protective measures it took, both before and after the inadvertent disclosure, to prevent production of the data at issue here. Walgreens contracted with FTI Consulting Inc., a data analytics firm, to assist with its

collection and production of dispensing data. *See* Ex. 3, Hamburger Aff. at 1-2. FTI took many steps not only to collect the data and ensure its completeness, but also to ensure it was properly de-identified and protected throughout the production process. *Id.* at 2-5. For example, to ensure the proper data was collected in time to meet the Court's March 2 deadline, FTI worked with a team at Walgreens for several weeks, writing targeted queries to collect the data from Walgreens' database. *Id.* ¶¶ 5-6. Initially, the team was unable to identify data prior to 2013. New code had to be written to pull additional data from other tables in the database. *Id.* ¶ 8. Then, to protect the data temporally, FTI wrote queries restricting the data to the Court-ordered timeframe. *Id.* ¶ 9. To ensure that all relevant data was collected for the stores at issue, FTI mapped DEA numbers to NABP numbers, as well as DEA numbers to store numbers. *Id.* ¶ 10. FTI reviewed store addresses, open/close date information, and relocation information, and confirmed all drugs dispensed during the relevant time period had a record of distribution into the stores in the ARCOS data. *Id.* ¶ 11.

To ensure that patient information was de-identified, FTI replaced all patient identifiers with a new, masked identification number. *Id.* ¶ 13. To ensure the dispensing data was protected in transit, and to prevent inadvertent disclosure to unauthorized users, FTI sent the data to Plaintiffs by encrypted hard drive, with a password provided separately by counsel, and chain of custody forms requested from all parties handling the protected data. *Id.* ¶ 14. FTI also requested return of the hard drives following Plaintiffs' upload of the data, and will destroy them in accordance with NIST standards. *Id.*

Collection, protection, and production of this data was time-consuming and burdensome. *See generally id.* It was conducted on a short timeframe due to the deadlines set by the Court over Walgreens' objections. Despite all best efforts, and the numerous safeguards that FTI put in

place, an error by FTI resulted in the inadvertent production of data from prior to 2006. Specifically, a date restriction was removed from a query in order to conduct quality control checks on the data, and that restriction was not added back after the check was completed. *See id.* ¶¶ 15-17. Walgreens attempted to claw the data back the same day that counsel realized the inadvertent production. Walgreens has taken all necessary steps to warrant a clawback. *See Heriot*, 257 F.R.D. at 660-661(allowing clawback of privileged documents where the "multi-step process Plaintiffs used to produce the Sequestered Documents … entailed reasonable precautions to prevent disclosure" and disclosure would have been avoided but for a vendor error).

Finally, the potential harm from further disclosure of this data significantly outweighs any benefit to Plaintiffs from receiving it. The Court has already determined that dispensing data prior to 2006 is outside the scope of discovery permitted by Rule 26. *See* Dkt. 3055 at 4 n.2 (limiting discovery of dispensing data to 2006 to the present based on Rule 26(b)(1)'s proportionality standard). During the meet-and-confer process preceding this motion, Plaintiffs did not even attempt to explain how data that the Court had previously ordered was not even discoverable was now somehow necessary to the prosecution of their claims. It is clearly not.

CONCLUSION

While the relief Walgreens seeks is necessary to protect the medical privacy interests of patients across Cuyahoga and Summit Counties, it can result in no hardship to Plaintiffs—applying, as it does, only to highly sensitive information that the Court has already ruled is outside the scope of permissible discovery. There is good cause for entry of a protective order requiring Plaintiffs to destroy the inadvertently produced dispensing data from prior to 2006, to confirm that they have done so, and to refrain from using any of that data moving forward.

Dated: March 18, 2020

Respectfully submitted,

By: /s/ Kaspar J. Stoffelmayr
Kaspar J. Stoffelmayr
Katherine M. Swift
BARTLIT BECK LLP
54 West Hubbard Street
Chicago, IL 60654
Phone: (312) 494-4400
Fax: (312) 494-4440
Email: kaspar.stoffelmayr@bartlitbeck.com
Email: kate.swift@bartlitbeck.com

Alex J. Harris
BARTLIT BECK LLP
1801 Wewatta Street, 12th Floor
Denver, CO 80202
Phone: (303) 592-3100
Fax: (303) 592-3140
Email: alex.harris@bartlitbeck.com

Counsel for Defendants Walgreen Co. and Walgreen Eastern Co.

CERTIFICATE OF SERVICE

I, the undersigned, hereby certify that the foregoing document was served via the Court's ECF system to all counsel of record on March 18, 2020.

/s/ Kaspar J. Stoffelmayr
Kaspar J. Stoffelmayr

Counsel for Walgreen Co., and Walgreen Eastern Co..